

WHAT IS CLAIMED IS:

1. A system, comprising:

5 a server cluster, comprising:

a plurality of server nodes, wherein each server node comprises:

a server container;

10 one or more applications configured to execute within the server container; and

15 a Java Data Object (JDO) persistence manager configured to detect changes to application state data and to persist the application state data; and

a persistent data store coupled to the cluster, configured to store application state data of the one or more applications;

20 wherein in response to a change in application state data, the persistence manager is configured to persist only changed application state data to the persistent data store.

25 2. The system as recited in claim 1, wherein the persistence manager is configured to persist only mutated application state data to the data store, only in response to mutation of the application state data.

30 3. The system, as recited in claim 1, wherein the application state data comprises hypertext transfer protocol (http) session data.

4. The system, as recited in claim 1, wherein the application state data comprises a session bean.

5 5. The system as recited in claim 1, further comprising a JDO-style write barrier configured to detect mutation of the application state data.

6. The system as recited in claim 1, wherein one or more of the applications is configured to function as a distributed application across two or more of the server
10 nodes.

7. The system as recited in claim 1, wherein the plurality of server nodes is configured to detect the failure of a cluster node and recover sessions from a failed node by accessing session state data from the persistent data store.

15

8. The system as recited in claim 1, further comprising a non-sticky load balancer configured to distribute session requests to server nodes based on server workload, wherein the persistence mechanism is configured to synchronize session data to the persistent store.

20

9. A system comprising:

an application server, comprising;

25

an application server container;

one or more applications configured to execute within the application server container; and

a Java Data Object (JDO) persistence manager configured to detect changes to application state data and to persist the application state data; and

5 a persistent data store coupled to the application server, configured to store application state data of the one or more applications;

wherein in response to a change in application state data, the persistence manager is configured to persist only changed application state data to the persistent data store.

10

10. The system as recited in claim 9, wherein the persistence manager configured to persist only mutated application state data to the data store, only in response to mutation of the application state data.

15

11. The system, as recited in claim 9, wherein the application state data comprises hypertext transfer protocol (http) session data.

20 12. The system, as recited in claim 9, wherein the application state data comprises a session bean.

13. The system as recited in claim 9, further comprising a JDO-style write barrier configured to detect mutation of the application state data.

25

14. A method, comprising:

a Java Data Object (JDO) persistence manager detecting an access to application state data;

30

the persistence manager determining whether the access alters the application state, in response to said detecting; and

5 the persistence manager persisting only the elements of the application state that are changed by the access to a persistent store, if the access alters the application state.

15 15. The method, as recited in claim 14, wherein the persistence manager persisting comprises persisting only mutated application state data to the data store, only in response to mutation of the application state data.

16. The method, as recited in claim 14, wherein the application state data comprises hypertext transfer protocol (http) session data.

15 17. The method, as recited in claim 14, wherein the application state data comprises a session bean.

20 18. The method, as recited in claim 14, wherein said determining is performed by a JDO-style write barrier configured to detect mutation of the application state data.

19. The method, as recited in claim 14, wherein said application state data comprises state data for one or more applications configured to function as a distributed application across two or more server nodes of a cluster.

25 20. A method, comprising:

detecting a failure of a node in a server cluster;

selecting one or more surrogate nodes from the remaining functional nodes in the cluster to take over the sessions of the failed node in response to said detecting;

5 the surrogate nodes accessing session state data for the sessions of the failed node from a persistent store in response to said selecting; and

resuming processing of the sessions of the failed node by the surrogate nodes based on the session state data from the persistent data store.

10

21. The method as recited in claim 20, wherein the persistent data store is accessible to all nodes of the cluster.

22. The method as recited in claim 20, wherein the plurality of server nodes
15 comprising the cluster is configured to detect the failure of a cluster node and each node of the cluster is configured to recover sessions from a failed node by accessing session state data from the persistent data store.

23. The method as recited in claim 20, wherein each node of the cluster is
20 configured to persist only changed session state data for each session comprised in that particular node in response to any change in the session state.

24. A computer-accessible carrier medium comprising program instructions,
wherein the program instructions are computer-executable to implement a Java Data
25 Object (JDO) persistence manager configured to:

detect an access to application state data;

30 in response to said detecting, determine whether the access alters the application state; and

if the access alters the application state, persist only the elements of the application state that are changed by the access to a persistent store.

5 25. The computer-accessible carrier medium as recited in claim 24, wherein the JDO persistence manager is configured to persist only mutated application state data to the data store, only in response to mutation of the application state data.

 26. The computer-accessible carrier medium as recited in claim 24, wherein
10 the application state data comprises hypertext transfer protocol (http) session data.

 27. The computer-accessible carrier medium as recited in claim 24, wherein the application state data comprises a session bean.

15 28. The computer-accessible carrier medium as recited in claim 24, wherein a JDO-style write barrier detects mutation of the application state data.

 29. The computer-accessible carrier medium as recited in claim 24, wherein said application state data comprises state data for one or more applications configured to
20 function as a distributed application across two or more server nodes of a cluster.

 30. A computer-accessible carrier medium comprising program instructions, wherein the program instructions are computer-executable to:

25 detect a failure of a node in a server cluster;

 select one or more surrogate nodes from the remaining functional nodes in the cluster to take over the sessions of the failed node in response to said
30 detecting;

 access current session state data for the sessions of the failed node from a persistent store in response to said selecting; and

resume processing of the sessions of the failed node by the surrogate nodes based on the session state data from the persistent data store.

5 31. The computer-accessible carrier medium as recited in claim 30, wherein the persistent data store is accessible to all nodes of the cluster.

 32. The computer-accessible carrier medium as recited in claim 30, wherein the plurality of server nodes comprising the cluster is configured to detect the failure of a
10 cluster node and each node of the cluster is configured to recover sessions from a failed node by accessing session state data from the persistent data store.

 33. The computer-accessible carrier medium as recited in claim 30, wherein each node of the cluster is configured to persist only changed session state data for each
15 session comprised in that particular node in response to any change in the session state.